量子コンピュータ時代に向けた暗号の在り方検討タスクフォース（第２回）
議事概要

１．日時
令和元年９月６日（金）10:00～12:00

２．場所
経済産業省別館11階　1111各省庁共用会議室

３．出席者（敬称略）
構成員：松本勉、宇根正志、國廣昇、高木剛、松井充、松本泰、満塩尚史
オブザーバ：岩田哲、徳永竜一、久山純也、岡野孝子、足立直、内山諒子、荒木美敬、
土本雄介、野口信、林巧、藤森英俊、中村佳憲、衛門愛子、花岡悟一郎
事務局：（総務省）赤阪晋介、梅城崇師
（経済産業省）鴨田浩明、上田翔太
（国立研究開発法人情報通信研究機構（NICT））野島良、盛合志帆
（独立行政法人情報処理推進機構（IPA））神田雅透

４．議事
（１）前回議事概要の確認について
（２）耐量子計算機暗号の扱いについて
（３）軽量暗号の動向について
（４）軽量暗号等の扱いについて
（５）その他

５．配付資料
資料１　第１回会合議事概要（案）
資料２　耐量子計算機暗号の扱いについて
資料３　岩田先生提出資料
資料４　軽量暗号等の扱いについて

６．議事概要
６．１．開会
松本勉座長から開会の宣言があり、岩田オブザーバの出席について説明があった。

６．２．議事
（１）前回議事概要の確認について
資料１の第１回会合議事概要（案）について確認が行われ、原案のとおり承認された。

また、宇根構成員より、同構成員も著者の一人として令和元年８月30日に公表された日本銀行金融研究所のディスカッションペーパー「量子コンピュータによる脅威を見据えた暗号の移行対応」について説明が行われた。主な質疑は以下のとおり。

松本泰構成員：P27の図表A-1に、鍵長2048ビットのRSA暗号が量子コンピュータによって解読されうる時期の試算がある。CRYPTRECにおいても議論のたたき台になるのではないか。

高木構成員：第１回会合で「Interface」を引用して「量子コンピュータの規模予測」を示したが、この図は更に傾斜を考慮して考えたものか。

宇根構成員：然り。既存の資料を活用し、誤り訂正能力も含めて場合分けして作成したものである。ワーストケース側に寄せた試算である。

國廣構成員：誤り率としている0.5%・0.01%は何を指しているか。

宇根構成員：誤り率は、既存の量子ゲート型コンピュータで発生している0.5%程度の場合と、既存論文で今後の目標とされている0.01%を設定している。なお、量子ビット数の増加に伴い誤り率が上昇すると考えられるが、ワーストケースとして誤り率の上昇は発生しないこととしている。

國廣構成員：量子ビット数以外にも計算時間などの指標もありえるため、量子ビット数だけに絞るのはよくないのではないか。

宇根構成員：どのように考えていくべきか引き続き検討していきたい。

満塩構成員：暗号移行の話として、「アクセス制御の強化」とは、アクセス制御を強化することか、それともアクセス制御を正確に使うということか。

宇根構成員：ICカードによる入退室管理システムなどで使用されている場合には、耐量子計算機暗号に切りかえて強化することを強化と呼んでいる。

一方で、バイオメトリクスの場合などで既存の技術を活用して運用を手厚くするという方法もありえると考えている。

満塩構成員：その意味では、適切にアクセス制御を利用するという趣旨か。

宇根構成員：然り。そのような場合もある。

満塩構成員：文書中にある「暗号処理部」とは何か。

宇根構成員：ランタイムで情報を読み出しながら処理する状況を想定している。ランタイム部分に問題があると、そもそも暗号システムの処理結果が信頼できないものになってしまうため、問題は大きいという考察である。

高木構成員：マイクロソフト社の「Open Quantum Safeプロジェクト」は、先週開催されたNISTの2nd PQC標準化会議でも議論になったハイブリッドシステムのことか。まだNISTの標準がないが、マイクロソフトが中心であるため、マイクロソフト派以外の人は使用しないといった問題はないか。

宇根構成員：ハイブリッドスキームについては、これをうまく組み込むことができれば、大規模量子コンピュータが実現する前から従来暗号と耐量子計算機暗号の両方で処理をすすめることができるため安心できるということである。

マイクロソフト社は一部の暗号ライブラリで先行して活動しているが、IEEEで標準化されRFCになっているハッシュベースの署名をNISTも今年中に標準に組み込む予定である。

マイクロソフト社の活動も、アマゾン等の主要ベンダーも参加し、Open SSL、Open SSH、Open VPNが対象になっている。実装性もそれなりにあると見込んでいる。

（２）耐量子計算機暗号の扱いについて

資料２に沿って、事務局より説明が行われた。主な意見等は次のとおり。

高木構成員：耐量子計算機暗号は量子コンピュータに対して安全だが、RSA暗号と楕円曲線暗号は量子コンピュータが大規模化すると安全ではなくなる。このため利用者視点として、量子コンピュータに対する安全性は考えない従来のリストと、量子コンピュータ時代の安全性を考えたリストとを分けることは良いアイデア。

今のCRYPTRECの暗号リストは、実用化や使用状況も考慮されるため、2023年の段階で普及している状況がなければ、リストではなく、ガイドラインにすることも良いアイデアである。

松井構成員：量子コンピュータの動向以上に、耐量子計算機暗号も今後の議論や攻撃手法の研究等によりどのようになるかわからない。リスト改定時に耐量子計算機暗号がリストとして載せる段階にはないかもしれないため、幾つかの可能性の一つとしてリスト群があるというフレキシブルな考えも必要である。

松本勉座長：資料中に「暗号リストと併せてリスト群として提示」とあり、「リスト群」とすると全てが「リスト」だと誤解されかねないが、この意味するところは、CRYPTREC暗号リストではなくて、ガイドライン等の別の文書とするということか。

事務局（総務省）：御認識のとおり、リスト群というのは語弊があるかもしれない。

松本勉座長：要するにサポーティングドキュメントのように、重要な資料であることが分かるように周知するといった趣旨かと思う。その意味で「リスト群」という言葉が使われており、ガイドライン等の中身をどうするかはこれからの検討。

宇根構成員：ガイドライン等の別の文書で扱うかどうかについては、何らかの形で文書としてまとめユーザーに示すようにすることが適切。

３ページの我が国における耐量子計算機暗号の開発・標準化については、研究が不十分な部分もあり、また、安全性等の検証にはまだ時間を要する状況。NISTの会議でも慎重に進めていく必要があるとなっており、CRYPTRECとしても慎重に検討する必要がある。量子コンピュータによって従来暗号が破られる状況がすぐに来るわけではないため、それまでに移行がスムーズにできるような体制を構築しておくことが重要。その意味で、ハイブリッドスキームのような観点でのサポーティングドキュメントの検討も有用ではないか。

國廣構成員：ガイドライン等の別の文書として扱うことについては、それが適当と思う。

耐量子計算機暗号の開発・標準化については、標準化というとCRYPTRECと関係がないようにみえる。国として何か考えること、やりたいことがあっての記載なのか。

事務局（総務省）：国として具体的な実施策が裏にあるものではなく、今回のタスクフォースにおいて、CRYPTREC暗号リストだけではなく、耐量子計算機暗号全体を見据えた幅広な議論を願って記載したものである。

事務局（NICT）：NISTから耐量子計算機暗号の標準化について、Round 2だけではなくRound 3まで実施することが発表になった。最速スケジュールだと2022年にはドラフト版が出る想定であったが、これにより２年は延びると想定されるため、CRYPTREC改定時期を考えるとガイドラインとする方針は適切かと思う。

松本泰構成員：2023年は、耐量子計算機暗号が実用的に利用できるようになっているかどうかに係らず非常に微妙な時期。RSA2048に相当する112bitセキュリティ暗号について、NISTのロードマップでは2030年には128bitセキュリティ暗号に移行すべきとしており、2023年というのは暗号を10年程度の保証をするとしたときに移行を始める時期。これを何らかの形で示す必要がある。データのライフサイクルも長くなっており、また、暗号がフレームワーク化しておりアルゴリズムが取り替えられるようなアーキテクチャが重要になっており、CRYPTREC暗号リストの立場を示さないと混乱するのではないか。

松本勉座長：現行のCRYPTREC暗号リストについて、耐量子計算機暗号をどのように位置付けるかという話と、現行リストに掲載された暗号をどのように移行するかという話は分けて考える必要がある。後者については、CRYPTRECの次期暗号リストに必要な情報を入力することが望ましいと思うが、耐量子計算機暗号については、別立てのガイドラインとすることが適当と考える。

ただし、日常的に耐量子計算機暗号の使用が必要となった場合は、電子政府推奨暗号リストに位置付けられるものと理解している。

高木構成員：2023年のリスト改定の際に、2030年以降のRSA2048移行について、耐量子計算機暗号への移行や鍵長の増加などについて、世界的な動きとともにリストに明記して利用者に示すことがよいのではないか。

また、CRYPTREC暗号リストへの掲載有無によって、企業の暗号開発への注力の度合いも変わるようであるので、日本の産業で使われるものは、ガイドライン等の形でも掲載し、状況にあわせて正式なリストに入れるような体制にしていくことは重要。

学術界としては、NISTのRound 2でも幾つかの攻撃手法が提案されており、標準化されたからといって未来永劫安全なわけではない。CRYPTRECでは監視体制のための人材もいるため、耐量子計算機暗号についての安全性を長期的に検討していく体制を維持していくことは非常に重要。

松本勉座長：2030年の移行については、民間でも準備がなされているかと思うが、それをCRYPTREC暗号リストの中でどのように位置付けるかは重要。

満塩構成員：NISTの動向も含めてサマリー的なものを整備するのがよいのではないか。

暗号移行について、従来はITシステムを５年程度で更改してきたため、そこで動く暗号アルゴリズムをどのように構築するかという話であったが、近年はクラウド利用が前提になりつつあり、開発もアジャイルやDevOpsといった方法で、暗号を切り替える部分が変わっていると感じている。これを踏まえた暗号移行の研究を始めてはどうか。また、量子コンピュータも自前で保有するというよりは、クラウド的に利用することが先行することも考えられ、その意味でもクラウドを意識したガイドラインの整備を考えてはどうか。

岩田オブザーバ：我が国における耐量子計算機暗号の開発・標準化について、量子コンピュータによって共通鍵暗号技術を突破できるものがあるという例示が報告されており、公開鍵だけでなく共通鍵についてもフォローしていくことが必要。

松本勉座長：AESはどうなるのか。

岩田オブザーバ：最近は、AESの安全性は思ったより低下しないといった論文が出ており、鍵長を倍にすれば使えるような認識である。

松本勉座長：AES-256を使用するのが現実的か。
岩田オブザーバ：AES-256があったとして、それを使用してどのようにデータを認証していくかは別の話であり、そのような点も含めて研究が進んでいくかと思う。
高木構成員：今年度の暗号解析WGで、共通鍵暗号に対する量子コンピュータの耐性の調査を実施している。
國廣構成員：暗号解析WGでは、こうした場合は安全ではないという形で、どうすれば安全かという形までは議論が進みそうになく、長期的視点で見ていくことになる。
高木構成員：その議論を踏まえて、2023年のリスト改定時に、共通鍵暗号に対しても量子コンピュータがどのような影響があるかを記述すべきである。
宇根構成員：満塩構成員からクラウドの話があったが、金融機関でもクラウドを使用する場合はどのように考えれば良いのか等の疑問が出ている。先ほどのディスカッションペーパーはオンプレミス環境が前提だが、クラウドは重要な論点である。
松本勉座長：今回の議論としては、耐量子計算機暗号については今後も動向をウォッチする必要があり、次期改定においては、暗号解析WGで検討した結果等も盛り込む必要があること。

また、耐量子計算機暗号については、ガイドライン等の別文書として取り扱うが、リスト本体から参照するなど何らかの形でその文書が重要だとわかる形式をとること。

それから、2030年やその先といった長期的な課題についても、CRYPTRECとしてどう考えていくかを考えていかなければならないこと。

そして、移行として、現在のCRYPTREC暗号リストは、仕様は参照しているが、パラメータまでは特定しないところもあるため、具体的にどのように考えるか参考になる情報も入れる必要がある。

（３）軽量暗号の動向について

資料３に沿って、岩田オブザーバより説明が行われた。主な意見等は次のとおり。

國廣構成員：軽量だから２の64乗でもよいわけでなく、112乗ないと議論に乗れないというように、高い安全性が要求されていることに驚いた。
宇根構成員：サイドチャネル攻撃耐性がDesign Requirementsとなっているが、処理時間が一定ということか。電力消費量一定みたいなことまで可能なのか。
岩田オブザーバ：そのような保護がしやすい設計をとるということがある。また、リンケージ・レジリエントというキーワードで、例えばモード等でデータ処理する際に中間状態の一部が敵の手に渡ったとしてもある程度の安全性が保たれる設計を目指しているというものがある。
宇根構成員：IoT機器等で使用すると、長期間使用し続けなければならないことがある。そうした大量のデータ処理についても、NISTでは考慮しているのか。
岩田オブザーバ：NISTでは、２の50乗バイト以上の暗号が処理できるよう規定しており、想定している大部分のユースケースはこの処理量で対応可能と考えられている。
松本泰構成員：軽量暗号はIoTで利用される暗号技術として非常に重要。一方で、例えばLightweight applicationsといったときに、これが具体的に何を指すのかとい

う共通コンセンサスは簡単に得られるものではない。また、IoT機器では省電力対応のため、小さなデータの送信時に128ビット暗号よりも送信時間が半分で済む64ビット暗号が、省電力対応の観点から欲しい場合もある。CRYPTRECの活動範囲としてはこうした応用層の話は見えにくく、CRYPTRECでそこまで含めたコンセンサスが得られるものを作ることは難しいのではないか。

岩田オブザーバ：2017年にCRYPTRECで軽量暗号のガイドラインを作成した際に、想定する軽量暗号のユースケースを幾つか例示している。

松本勉座長：CRYPTRECでの取扱いについては次の議事で議論する。

國廣構成員：CAESARとNISTの標準化の関係はどのようになっているのか。

岩田オブザーバ：CAESARは学術コミュニティ手動であり、ポートフォリオに選ばれた何かの標準になるというわけではない。

また、CAESARは2014年に応募締切であったが、当時はユースケース分類がなく、AsconとACORNはLightweight applicationsとして提案されたわけではない。その意味では、NISTとしてもLightweightをするに機は熟したと判断した可能性はある。なお、AsconはNISTに提案されているが、ACORNは提案されていない。理由は不明である。

事務局（NICT）：NISTから発表されたRound 2候補から見えてくる、選定ポリシーのようなものはあるか。

岩田オブザーバ：初期不良が指摘されたアルゴリズムは選ばれていない。また、コメントが出ても収束していないものや議論中のものは残っている。NISTが選定した背景を今後コメントするとしているのでそれを待ちたい。

傾向としては、暗号学的置換に基づくものが有力のように見え、認証暗号とハッシュ関数との橋渡しが容易であるという点が挙げられる。

高木構成員：NISTのDesign Requirementsにおいて実装性能等があったが、ハードウェア・ソフトウェアのテスト環境をNISTは指定しているのか。

岩田オブザーバ：指定している。CAESARでGMUがハードウェア評価用のプラットフォームを出しており、これに準じたものを使うとしている。ソフトウェアも名前が挙がっていたように思う。

高木構成員：サイドチャネル攻撃耐性についてはどうか。

岩田オブザーバ：提案者やコミュニティに任されているかと思う。

松本勉座長：CAESARは必ずしも軽量暗号だというわけではなく、認証暗号というカテゴリで公募して進んできて、その中には軽量性のあるものも入っている。その一部はNISTの軽量暗号標準化プロジェクトにも応募されているということか。

岩田オブザーバ：その理解である。CAESARポートフォリオの中でAsconという暗号がNISTのRound2にも残っている。

（４）軽量暗号等の扱いについて

資料４に沿って、事務局より説明が行われた。主な意見等は次のとおり。

＜軽量暗号について＞

松井構成員：「軽量暗号とはそもそも何か」の議論が難しい。

NISTでもAESベースのものが結構あるが、AESのモードを工夫して軽量にしている。一方でAESは128ビットブロック暗号として既にCRYPTREC電子政府推

奨暗号リストに掲載されている。AESのモード次第で軽量暗号になるとすれば、軽量暗号の定義付けをどのように考えていくのか、公的な文書としてどのように考えるのかは難しく、議論が必要。

松本勉座長：2017年に軽量暗号のガイドラインを作成した際は、AESを基準としてそれに比べて何らかの点で軽量性があるということだったかと理解している。

岩田オブザーバ：そのとおりであり、電力等でAESより優位性があるものを軽量暗号と呼んでいた。また、ブロック暗号単体で話す場合はよいが、実際に使用する場合はブロック暗号単体として利用するわけではないため、松井構成員が述べられたような齟齬が生じる。

松本勉座長：軽量性をどのように取り扱うかという議論が必要との指摘であり、その通りかと思う。

松本泰構成員：「安全性を一部トレードオフした」という記載があるが、トレードオフではなく、何らかの制約の下で安全性を確保したものが軽量暗号であるとの認識。

松本勉座長：個々に状況が異なるが、「安全性を確保した」というと、制約がない場合に比べて保証や確認の手厚さが劣るのではないか。

岩田オブザーバ：先ほどのNISTのDesign Requirementsをみても要求自体のレベルが非常に高く、一概に安全性が損なわれているとは思えない。

利用環境が制限されているため、一般的なリストとは変えることは選択肢としてはあり得る。ただ、安全性のトレードオフは、該当するものとしないものとがある。

事務局（NICT）：NISTのDesign RequirementsはCRYPTREC暗号リストとしても参考になる。

松本勉座長：CRYPTRECにおいて軽量暗号の定義をする際に、ほかのアクティビティとして出ている基準等はとても参考となる。

現行の暗号リストには、想定しているアプリケーションであるだとか、データ取扱に関する要件は入っておらず、個々の暗号について安全性や利用実績を見ている。軽量暗号については、政府調達等でも使用されるものについて、どれを選んだらよいかという参考になる情報が整理されていることが重要。

次期改定リストに軽量暗号というカテゴリがいきなり入るということではなく、現行のリストとは別立てで整理する議論が望ましい。その際、現行の「ガイドライン」だと単なる参考文書のようにも見えるため、位置付けを議論する必要がある。

高木構成員：現行の暗号リストとは設計思想や安全性の評価指標が違うため、軽量暗号が非常に普及したとしても、セキュリティと使用環境をセットにして明示し、セキュリティが通常とは異なるということがわかるように別リストとしたほうがよい。

宇根構成員：先ほどの軽量暗号の定義が難しいという点については同意見。

現行のリストにおいて軽量なものであれば、電子政府推奨暗号リストに64ビットブロック暗号はなく、推奨候補暗号リストはMISTY1等があるといったように当て込みは可能であるが、利用者側の要求条件等は別文書にするほうが現実的である。

松本勉座長：リストへの位置付けについて幾つか御意見を頂戴した。耐量子計算機暗号も

同様であるが、対象を多くすれば、それだけ評価体制も整えなければならず、投入できるリソースも含めて検討していく必要がある。

＜高機能暗号について＞

國廣構成員：高機能暗号については、従来のリストのようにリストアップすることは難しい。新しい方式が日々提案され、改良もされている。このタイミングで特定のものをリストに挙げて固定化することは難しく、方式を決め打ちにすることは現状にそぐわないのではないか。

満塩構成員：軽量暗号や高機能暗号について、利用者側視点からは、ユースケースや制約がわかればよい。現行のリストだとそうした点ができていない理解であり、そこをどのようにわかりやすく書けるかがポイントになる。

宇根構成員：高機能暗号のキラーアプリケーションは、既存の暗号でも実現できなくはないが、高機能暗号の使用によって、ユーザビリティやコスト的な有効性が高まる等の話になるのかと思う。そうすると、既存のシステムを構築し直してまでコスト的にメリットがあるのか、使い勝手が良くなるのか等の内容になるため、個別の事象に特化しないと議論が深まらない。現時点では、様々なケースで議論を深めないとリストの取扱いについて議論するのは難しい印象がある。

松本勉座長：高機能暗号についても研究が盛んに行われており、耐量子計算機暗号より先に高機能暗号が普及する印象を持っている。耐量子計算機暗号についての議論は着々と進める必要はあるが、高機能暗号についても利用が一気に広まるまでに関連ドキュメントの整備を進めておく必要がある。

松井構成員：高機能暗号はアルゴリズムよりも更に上位レイヤーの概念。これをCRYPTREC暗号リストの観点からどのように捉えるかは非常に難しい観点。応用側によっているからこそ価値のある高機能暗号について、高機能暗号とは何かといった議論から深めていく必要がある。

松本泰構成員：耐量子計算機暗号も軽量暗号も高機能暗号も同様だが、CRYPTREC暗号リスト以外は使用不可とすることが、暗号技術を利用したイノベーションを阻害する可能性が出てくることが大きな問題。その点について、どのようにバランスを取るかがCRYPTREC暗号リストに望まれている。

高木構成員：高機能暗号が普及して使われ始めたときに、どの程度安全なのかをCRYPTRECで議論することは非常に価値がある。その結果についてどのような形になるかわからないが、発表することで、安心して使ってもらえるようになる。

６．３．閉会

事務局から次回は12月頃の開催を予定しており、詳細な日程、場所等については、別途連絡する旨の説明が行われた。

以上